Web Service Security in an Air C2 System

Dr. Mutlu Uysal
Senior Scientist Head
NATO C3 Agency
Production Division - CAT4
C2 Systems Group
Tel: +31 (0)70 374 3735

E-Mail: Mutlu.Uysal@nc3a.nato.int

Mr. Jean-Paul Massart
NATO C3 Agency
Production Division - CAT4
C2 Systems Group
Tel: +31 (0)70 374 3731

E-mail: Jean-Paul.Massart@nc3a.nato.int

ABSTRACT

With the development in information and network technologies, more systems began to be connected to each other in a network environment and interoperability between them became a crucial requirement. In order to achieve this interoperability, systems should be adapted to more net-centric solutions where the information is shared, rather than stovepipe approaches where the information is for local use only. Although net-centric solutions require sharing the information among different systems in the enterprise, this information should be shared with the trusted parties only but not to every system in the network. Therefore there should be enterprise level security mechanisms which ensure that information is securely shared among the providers and consumers. This is one of the most important criteria to meet for the utilization of network enabled capability in a trusted manner.

This paper will focus on the experiences of NC3A C2 team from its Network-Enabled Capability (NEC) studies with the Integrated Command and Control (ICC) capability and will aim to share the lessons learned with the community especially related to the security issues.

1.0 INTRODUCTION

The philosophy underlying "network enabled capability" is to provide the right information, at the right place and at the right time to increase the operational effectiveness in a multi-functional and multi-national environment such as a NATO domain. NEC is recognized as being essential for meeting future challenges in the Trans-Atlantic environment. Through NEC, nations and NATO seek to capitalize on the use of new development approaches to improve operational effectiveness through the networking of their operational capabilities. The development of a NATO NEC (NNEC) is viewed by many nations as the most effective way for their Nation to be able to use their own investments to the full in supporting future coalition operations [1].

In the current state-of-the-art, this network-enabled capability is achieved by integrating different systems within a Service Oriented Architecture (SOA). SOA is a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains.

Web services are today's most widely used and popular implementation of a service oriented architecture. Note that SOA is the architectural style, whereas the web services are the current most popular implementation of this architecture [2]. Over the past few years, more and more systems began to be interoperable with each other using web service technology.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2010	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Web Service Security in an Air C2 System	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **NATO C3 Agency Production Division - CAT4 C2 Systems Group**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT
With the development in information and network technologies, more systems began to be connected to each other in a network environment and interoperability between them became a crucial requirement. In order to achieve this interoperability, systems should be adapted to more net-centric solutions where the information is shared, rather than stovepipe approaches where the information is for local use only. Although net-centric solutions require sharing the information among different systems in the enterprise, this information should be shared with the trusted parties only but not to every system in the network. Therefore there should be enterprise level security mechanisms which ensure that information is securely shared among the providers and consumers. This is one of the most important criteria to meet for the utilization of network enabled capability in a trusted manner. This paper will focus on the experiences of NC3A C2 team from its Network-Enabled Capability (NEC) studies with the Integrated Command and Control (ICC) capability and will aim to share the lessons learned with the community especially related to the security issues.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**10**	

Since web services have been very popular in recent years, a lot of research has been done on this topic including security related issues [3]. Web service security can be applied on two major levels which are “transport” and “message”. In the transport level security, all the data is sent in an encrypted way between the provider and the requestor on the network. This is a point-to-point security mechanism which provides data integrity and confidentiality. It can also be used together with a basic authentication method such as username/password token to provide a basic security solution for web services. However, it has two major drawbacks. Firstly, it provides a point-to-point solution which becomes an issue when one or more intermediaries exist between the requestor and the provider. Secondly, it does not support digital signatures, so that communicating partners can’t prove later that the data were really sent by each other.

On the other hand, in the message level security, encryption and signatures are applied to the message itself. It can either encrypt/sign the whole message or parts only. The messages can be stored and used later for non-repudiation if there is a disagreement. It does not only propose a point-to-point solution but also an end-to-end solution to support intermediary nodes in the middle of the traffic between the providers and consumers.

This paper is prepared to share the experiences and lessons learned of NC3A C2 team related to security issues from its NEC studies with the Integrated Command and Control (ICC) capability. ICC is an Integrated Command, Control, Communications and Intelligence (C3I) environment that provides information management and decision support to NATO Combined Air Operations Centre (CAOC) level air operation activities during peacetime, exercise and wartime.

Since NEC is recognized as being essential for meeting future challenges in the Trans-Atlantic environment [1], ICC has been involved in many studies to utilize this concept in recent years. Considerable work has been achieved by the ICC team to apply this concept to a command and control system to improve the operational effectiveness through its usage. ICC has both developed services in line with NEC concepts as a service provider and also consumed the available services from the NATO network as a service consumer.

Security is one of the most important concerns of ICC when providing its data to the other systems. This paper will include the solutions that are applied to ICC to make it more secure in providing its data using web services. It will first summarize the current security solution that is applied to ICC web services together with its advantages and disadvantages. Then, it will propose an enhanced security solution in order to address the weaknesses of the current solution in future.

In summary, the utilization of NEC by NATO systems is recognized as being essential for meeting future challenges and needs in the Trans-Atlantic environment. Considerable investment and work has been achieved in recent years to capitalize on its usage to improve operational effectiveness in NATO. This paper will focus on the experiences of NC3A C2 team from its NEC studies with the ICC capability and will aim to share the lessons learned with the community especially related to the security issues.

2.0 BACKGROUND

This section will provide some basic background information related to web services and security. It is suggested to refer to the papers in the references for further detailed information about these technologies.

2.1 Web Services Basics

A web service is a collection of protocols and standards which enables integration between heterogeneous systems. Web services provide a standard means of interoperability between different software

applications, running on a variety of platforms and/or frameworks. The most common web services are XML-based information exchange systems using a Web Services Description Language (WSDL) to describe its services [2].

The typical usage of web services is synchronous request-response, where clients simply make a request and get the response from the server. For most systems, this approach is sufficient to implement and interface with other systems. The service registry component may also be used to publish the service interfaces by the producers and to search the available services by the consumers (See Figure 1).

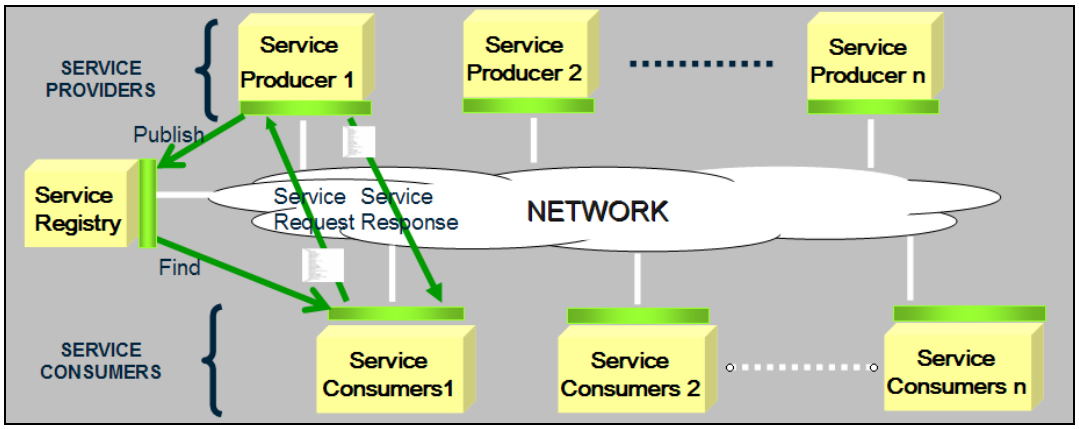

Figure 1: A Service Oriented Architecture Using Web Services

2.2 Security Basics

Fundamental elements of the security [4] are as follows:

Authentication: Verifying the identity of a user, process, or a system, before allowing to access to the resources in an information system.

Authorization. The permission to use a resource or to perform an action that is requested from the application.

Integrity. The property where data has not been altered in an unauthorized manner while in storage, during processing, or in transit. This feature ensures that the receiver of the message gets the same information that is sent by the sender without any data tampering.

Non-repudiation. Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Confidentiality. Preserving authorized restrictions on information access and disclosure. This feature will ensure that "unauthorized" parties do not get the opportunity to view the message.

Privacy. Restricting access to subscriber or relying party information in accordance with the organization policy.

In the next section, the relation between these fundamental security elements and the web services will be explored under "Web Service Security" heading.

2.3 Web Service Security

The widespread use of Web Service for providing business level solutions puts a great emphasis on security issues of the developed applications. In the past, the most diffused approach for handling authentication credentials was to use custom SOAP headers to transmit user credentials. Starting from 2000's, many supplemental standards for guaranteeing security features in Web Services have been proposed and collected under the WS-Security specification. This specification was released at the beginning of the 2006 by the OASIS Technical Committee.

WS-Security proposes a standard set of SOAP extensions that can be used when building secure Web services to provide confidentiality, integrity and authentication, non repudiation [5]. These enhancements include functionality to secure Simple Object Access Protocol (SOAP) messages through XML digital signature, confidentiality through XML encryption, and credential propagation through security tokens. The specification includes descriptions of how to include the security tokens and keys such as text-based tokens like the username/password, binary security tokens like X.509 and Kerberos tickets or signature and encryption keys.

2.3.1 Web Service Security Standards

Some standards related to web service security are summarized below. For further information, the readers can refer to the reference [6].

- Secure Socket Layer (SSL) and Transport Layer Security (TLS): This provides a basic level of security at the communication level.
- XML Encryption and XML Signature: These are the most fundamental standards that specify how to represent encrypted and signed XML data.
- WS-Security: This standard specifies how to represent encrypted and signed parts of a single SOAP message.
- WS-SecureConversation and WS-Reliability: The former specifies how to represent information related to the exchange of multiple secured SOAP messages, while the latter is focused on message delivery guarantee.
- Security Assertion Markup Language (SAML): SAML is an XML-based framework for exchanging security information in the more general form of security-related assertions about subjects.
- WS-Policy, WS-PolicyAssertion, WS-Policy Attachment, and WS-Security Policy: The first standard provides a general framework for expressing different kinds of security policies. The second standard specifies generic security assertions. The last two standards specify the protection requirements for SOAP messages and how to represent them at SOAP message level.
- eXtensible Access Control Markup Language (XACML) and XACML Profile for Web services: These standards provide a model and a language to express access control policies that can be applied to Web services as well as to other resources.
- Extensible rights Markup Language (XrML). This standard addresses how to express and enforce access control and information dissemination policies.
- XML Key Management Standard (XKMS): It specifies standard services interfaces and protocols for the management of cryptographic keys.
- WS-Trust: It specifies and describes the model for establishing and coordinating trust relationships between multiple parties.
- WS-Federation: It is built on all previous specifications to specify how to broker and manage heterogeneous, federated trust contexts.

2.3.2 Web Service Security Approaches

There are three alternative approaches for securing web services, which are transport-level security, message level security and the mixed mode:

1. Transport-Level Security

In this approach, the security credentials are applied at the transport level therefore all messages between the sender and the receiver are not visible to any intruders. This approach also works effectively on point-to-point scenarios. It is difficult however to implement transport-level security when there are multiple routing mechanisms to multiple recipients. Multiple gateways will expose the messages to intruders when the message is transferred from one SSL provider to another. This feature will make the transport-level security unrealistic for nonpoint-to-point scenarios. On the other hand, hardware accelerators can be used to achieve quick response times under this model. Transport-level security is also considered for high-throughput and faster response times because of this feature. Transport-level security provides mechanisms to authenticate both the service and the client so they adhere to confidentiality, integrity, and authorization [7].

2. Message-Level Security

Message-level security relies on securing the message itself rather than securing the communication channel. The authentication, authorization, integrity, and confidentiality are met by applying this approach. It does not rely on the transport mechanism to provide security. The message level security provides an end-to-end security context for the enterprise. It also works well with multiple hops and multiple recipients. Since it does not rely on the transport layer, the message headers can be expanded to implement multiple security assertions. This also enables the building of a federation of services. Persistence of message headers enables the utilization of integrity and confidentiality checks. Rich claims (SAML, Custom Tokens, WS-Trust, and so on) are also supported in message-level security. Multiple authentication mechanisms can be utilized at different gateways. However, the downside of this approach is that the message can get considerably larger because of additional header information. Therefore, the throughput will be slower than transport-level security [7].

3. Mixed Mode

Transport level security is faster than message level security, but they have limited credential types (like no SAML tokens). The message-level security has a richer set of credentials however because of XML serialization and de-serialization, they are slower than transport mode. It is required to have a rich set of claims and at the same time be optimized to the wire. Mixed mode offers the rich claims and federation advantages that message-level offers. It supports multifactor authentication using rich credentials. Therefore, mixed mode offers a secure and fast option to transmit data between services and clients. Mixed mode will perform the integrity and confidentiality at the transport level. The authentication and the authorization takes place at the message level [7].

3.0 ICC AND NEC ARCHITECTURE

ICC is an Integrated Command, Control, Communications and Intelligence (C3I) environment that provides information management and decision support to NATO Combined Air Operations Centre (CAOC) level air operation activities during peacetime, exercise and wartime. The ICC provides functional support for the most critical Air C2 functions at the CAOC level, such as Planning and Tasking, Air Task Order (ATO)/Air Task Message (ATM) generation, and Current Operations (Defensive and Offensive section).

The standard ICC architecture is a "3-tier architecture" which includes a database server based on an Oracle database, a COSI layer as the middle-tier (containing business logic) and finally a client application running on the desktop. ICC clients open a CORBA connection to the COSI layer to perform get/set operations. In the enhanced version of ICC for NEC, a web service layer, called WISI, is added on top of the COSI layer (See Figure 3). With the help of this additional layer, it becomes easier to reach ICC data for all other 3rd party applications using standard protocols such as HTTP, SOAP and XML. This new approach and capability provides a new mechanism for other systems to interoperate with ICC.

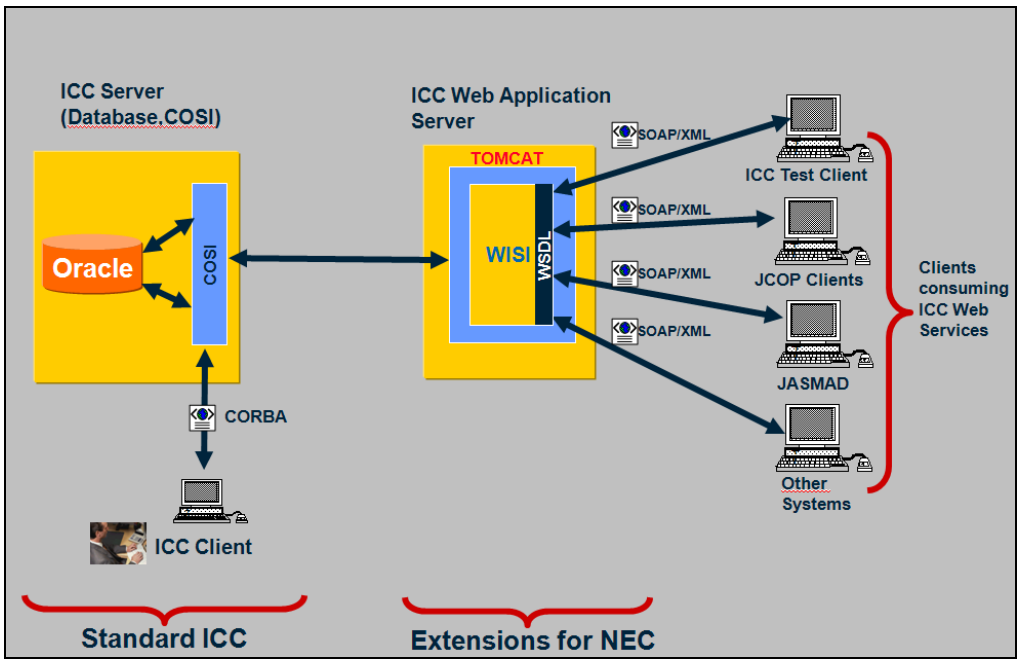

Figure 3. ICC Web Service Architecture

In the current architecture, TOMCAT is used as the web application container. Tomcat provides five different plug-ins to support various sources of authentication information such as:

- MemoryRealm - Accesses authentication information stored in an in-memory object collection, which is initialized from an XML document (conf/tomcat-users.xml).
- JDBCRealm - Accesses authentication information stored in a relational database, accessed via a JDBC driver.
- DataSourceRealm - Accesses authentication information stored in a relational database, accessed via a named JNDI JDBC DataSource.
- JNDIRealm - Accesses authentication information stored in an LDAP based directory server, accessed via a JNDI provider.
- JAASRealm - Accesses authentication information through the Java Authentication and Authorization Service (JAAS) framework.

For each of these standard Realm implementations, the user's password (by default) is stored in clear text. In many environments, this is undesirable because casual observers of the authentication data can collect enough information to log on successfully and impersonate other users. To avoid this problem, the standard implementations support the concept of *digesting* user passwords.

Among these plug-ins, ICC web services uses “MemoryRealm” to provide basic authentication using username token with digested passwords. Transport-level security using “HTTPS” is also applied for confidentiality and integrity at the transport level. This approach provides a point-to-point solution between ICC and the individual consumers. This solution however does have some limitations when there are multiple routing elements in the middle.

In order to meet the future needs and challenges, it is planned to start using message level security mechanisms together with transport level security mechanisms complaint with OASIS web service security standards. Note that NATO has an ongoing effort to have some infrastructural services such as security, registry etc., which can be used by the functional services rather than implementing such core capabilities by themselves. ICC will also refer to these NATO core infrastructure services whenever they will be ready in future.

4.0 LESSONS LEARNED BY NEC STUDIES

ICC has been involved in many NNEC studies with both NATO and national command and control systems. Many valuable lessons were learned from each of these studies. This section summarizes some of these learned lessons and some challenges that are faced during these studies including security issues.

4.1 Towards Service Oriented Architecture

In the past, stovepipe systems were built, which performed their functions very well but were not interoperable with each other. There was a barrier in between the systems running at different domains such as air, land and maritime and even in between the different systems in the same domain. Over time we learned that, we should move our application infrastructure from an inefficient, inflexible model - with vertical, stovepipe applications - to a less expensive, enterprise-wide model that delivers a reusable suite of interoperable services as also shown in Figure 4.

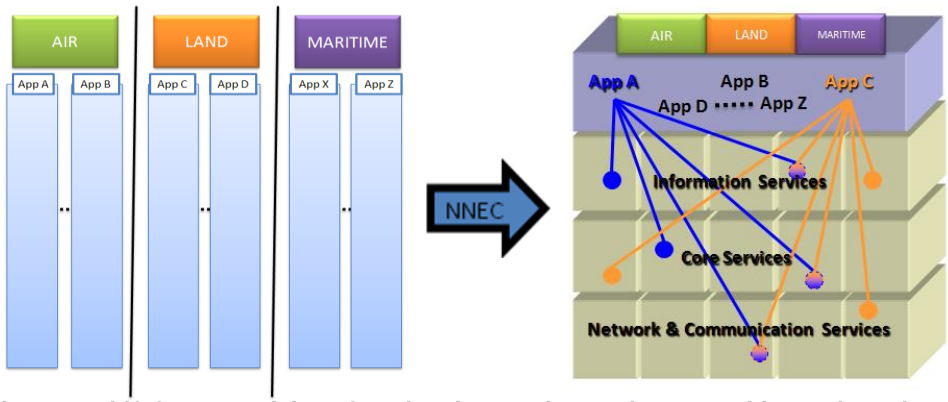

Figure 4. Shift from standalone functional stovepipes to interoperable service oriented systems.

This shift to NEC concepts offers many benefits by providing a natural decoupling between the services and the clients using these services. This decoupling results in fewer dependencies between systems. As a result of this, systems operating on different budgets, timeframes or schedules, can be changed without impacting each other. In other words, changes in one application will not force a change in another, which is also called “loose coupling”. Implementing loosely coupled integration approaches reduces the complexity and therefore the cost of integrating different heterogeneous systems. This enables us to build modular applications with more flexibility.

4.2 General Learned Lessons from the NNEC Studies

The learned lessons will be grouped under three sub-headings such as: service definition, quality of service and service provisioning.

Service Definition

- The web service interface should be well-defined to prevent misunderstandings and misinterpretations between the providers and consumers. Service contract must provide unambiguous information about what the service provides. Extra annotations for all defined elements and constraints about all possible data values should be added to the interface descriptions to achieve self-documented clear web service interfaces.
- Service granularity is very important in definition of the web service interfaces. Granularity is the extent to which a system is broken down into small parts. Fine-grained services address small units of functionality or data exchange whereas coarse-grained services encapsulate larger amounts of capability within a single interface. There should be a good balance on the granularity of the services which will result either larger amounts of data to be exchanged in a single call or many service calls each of which is returning a small amount of data. Each of these choices may fit well to different problem domains based on the requirements and the other variables.
- It should be preferred to reference to some commonly accepted models rather than defining new models whenever possible. Referencing to common models makes the job of the consumers easier. On the other hand, referring such a common model may cause loss of some data due to improper mappings between the real data model and the referenced one.

Quality of Service

- Quality of service issues should be considered as critical from the start until the end of projects. Some load-balance testing activities should be considered as part of the development process starting from the early phases.
- Applying some compression techniques for web services may help to minimize the bandwidth usage and decrease the transmission time of the XML messages over the network especially in wide area networks.
- Although it is a good practice to use web services for the flexibility that they offer for the interoperability across different platforms and different programming languages, in some cases, the use of native interfaces for internal tasks for performance matter may be needed.

Service Provisioning

- If the number of services available on the network increases, the need for a global service registry becomes vital to ease the configuration and enable dynamic binding between the producers and consumers. Although such a registry was not used in our experiments, NATO has an ongoing metadata and service registry project for this purpose, which will be a core component in future.
- Service orchestration helps to build business processes using basic services. There are a lot of commercial and free enterprise service bus tools for this purpose. These tools may be helpful for data transformations and may also provide some core service functionality like security, auditing and monitoring.

4.3 Learned Lessons from the NNEC Studies Related to Security Issues

Security is one of the most important criteria to handle for the utilization of network enabled capability in a trusted manner. Services are for sharing the data but it must be noted that the data should be shared with trusted parties only and not to every system on the network. There should be enterprise level security mechanisms which ensure that data is securely shared among the providers and consumers.

It is very important to note that security should be a core service in an enterprise. All the functional systems should use the infrastructure rather than implementing authentication and access control logic themselves. Core security services should be implemented separately from the service producers. Such an approach helps to standardize the use of security features in an enterprise which also helps to solve some of the interoperability problems due to incompatible standards.

SOA governance is very critical in order to have a standard approach across the enterprise. It refers to formal policies, processes, and procedures for development and management of services and business processes throughout the SOA lifecycle. Governance is required to define and enforce architectural, technical, and business policies to ensure the promise of SOA is realized [8]. A SOA Governance body is considered a key requirement for implementing a governance model in a SOA environment. Such a body interacts with both developers and end users by defining and addressing areas for governance such as service security, service registry, service lifecycles, service testing. It identifies processes and best practices for ongoing development and implementation, and provides the leadership and forum necessary for determining needs, SLAs, and dependencies [9].

In NATO, the NATO C3 Board (NC3B) has been given responsibility for NNEC Governance. NC3A is managing the implementation of SOA, in support of NNEC, under its role as the Implementation Authority for the Bi-Strategic Command Automated Information System (Bi-SC AIS). Security is one of the important elements of this governance effort.

The challenge with securing a SOA is that some services and applications already provide their own preferred security mechanisms. One application's security protocol may differ from the security protocol of another one with which it is communicating. The ultimate goal should be to have the integration between these applications with a minimal effort. The integration should be possible without needing to write extensive code, incur additional maintenance costs, or leave open holes that cause not to protect sensitive data.

There may be some cases where the two involved standard specifications are not always synchronized. Interoperability of different WS-Security implementation is crucial. For this reason, Web Services Interoperability Organization (WS-I) has developed the Basic Security Profiles to provide clarifications and constraints in order to enhance the interoperability of WS-Security implementations. It is strongly suggested to also refer to these profiles to have maximum level of interoperability.

An alternative approach to handle the security issues in an enterprise is to utilize enterprise service bus (ESB) products. Such products help to address security concerns at all levels starting from transport level to the application level. Policy-based enforcement allows access to services. ESB's can act as an intermediary and a single point of enforcement for policies that can be centrally governed. The maintenance of security policies becomes much more manageable as a result. These products also provide solutions that bridge multiple security protocols with minimal coding. Creating secure service-enabled processes for integration using ESB's as a central security bridge makes it easy to secure new and existing services, and to manage those services on an ongoing basis [10].

5.0 SUMMARY AND CONCLUSION

The utilization of NEC by NATO systems is recognized as being essential for meeting future challenges and needs in the Trans-Atlantic environment. A lot of investment has been accomplished and considerable work has been achieved in recent years to capitalize on its usage to improve operational effectiveness in NATO. ICC has also been involved in several studies with many NATO and national C2 systems to utilize this concept in recent years. All of these studies showed that web services offer a key enabler technology to share data and business processes between different systems in a loosely coupled way to achieve NNEC.

In this paper, we focused on the experiences of the NC3A C2 team from its NEC studies with the ICC capability and aimed to share the lessons learned with the community especially related to the security issues. As the requirements and technologies involved are still evolving, our studies on this concept will continue in the future.

6.0 BIBLIOGRAPHY

[1] NATO Network Enabled Capability Feasibility Study (NNEC FS), Volume II, Version 2.0, October 2005, NATO Unclassified

[2] W3C, World Wide Web Consortium, http://www.w3.org/2002/ws

[3] OASIS Reference Model for Service Oriented Architecture 1.0, Committee Specification 1, 2 August 2006

[4] Anoop Singhal, Theodore Winograd, Karen Scarfone, Guide to Secure Web Services, NSIT Special Publication 800-95.

[5] H. Labiod and M. Badra (eds.), New Technologies, Mobility and Security, 541–553, 2007 Springer.

[6] E. Bertino et al., Security for Web Services and Service-Oriented Architectures, DOI 10.1007/978-3-540-87742-4 4, Springer-Verlag.

[7] Chris Peiris, Dennis Mulder, Shawn Cicoria, Amit Bahree and Nishith Pathak, Implementing WCF Security, 2007, DOI 10.1007/978-1-4302-0324-7, 213-247.

[8] Greg Bjork (CEO WebLayers), SOA Governance Technical Exchange Meeting, The MITRE Corporation, 18 January 2007.

[9] Jeff Gold, "SOA Governance" Overview Brief, The MITRE Corporation, 5 January 2009.

[10] Jeff Davies, David Schorow, Samrat Ray and David Rieber, The Definitive Guide to SOA, Second Edition, 2008 pp. 225-264